Endpoint Security Using Biometric Authentication for Secure Remote Mission Operations

Authors:
John T. Donohue, NASA/GSFC Code 584, Real Time Software Engineering Branch, ISC, Greenbelt, MD 20771. 301-286-6149, john.t.donohue.1@gsfc.nasa.gov

Anna R. Critchfield, Computer Sciences Corporation (CSC) 7515 Mission Drive, Lanham, MD 20706. 301-805-3734; acritchf@csc.com

Purpose

We propose a flexible security authentication solution for the spacecraft end-user, which will allow the user to interact over Internet with the spacecraft, its instruments, or with the ground segment from anywhere, anytime based on the user's pre-defined set of privileges. This package includes biometrics authentication products, such as face, voice or fingerprint recognition, authentication services and procedures, such as: user registration and verification over the Internet and user database maintenance, with a configurable schema of spacecraft users' privileges. This fast and reliable user authentication mechanism will become an integral part of end-to-end ground-to-space secure Internet communications and migration from current practice to the future. All modules and services of the proposed package are commercially available and built to the NIST BioAPI standard, which facilitates "pluggability" and interoperability.

Problem

There are vast varieties of spacecraft users with different scope of authority. They include flight operations team (FOT), scientists, principal investigators (PI), mission planners and analysts. Within each group, user privileges and authority are further subdivided, for example, command controller and flight controller for the FOT or individual instrument for the responsible scientist or PI. The users' home "turf" is often located in different physical or geographical areas (countries, universities, offices, and personal residences). An individual user may be replaced or the user's assignment and corresponding privileges may change as a normal practice. All of these issues require that the Internet, which is a communication medium for spacecraft operations, be re-enforced with a highly reliable, configurable, and user-friendly end-user authentication solution. The proposed biometrics authentication via the Internet provides necessary functionality and attributes that facilitate end-point security authentication.

Proposed Solution

The proposed authentication solution uses unique biometric signatures, such as a user's unique face and fingerprint. Access is restricted to trusted users only. Traditional authentication solutions such as PIN, password/pass-phrase, even smart/magnetic/proximity cards and digital certificates do not guarantee that only a trusted user is allowed to access a secure network or web site. This solution combines the advantages of biometrics and the Internet to offer the most secure and efficient method to verify user IDs with the least amount of capital expenditure, integration effort, maintenance, and risk. Several products have been demonstrated to Code 584, including Etrue Systems (www.etrue.com).

Operational Scenario

Users request registration and verification of their face and/or finger from their client PCs to the destination server that they want to access in a secure manner. The request is sent via a secure network (Virtual Private Network) to an authentication processing system performed by an Authentication Services Provider (ASP). The ASP administers a secure server and performs registration, verification, logging audit trail, database maintenance, and other authentication business logic and services. The authorized user can then access the requested destination server. The authentication process is seamless and works in a few seconds, similar to the credit card approval process at a retail store. This is a modular plug-and-play solution. The client's biometric signature capture devices (camera, finger scanner) can be changed and upgraded with new devices with no significant impact on the ASP server. The ASP server can be built and maintained in house (e.g., Goddard) or these services can be procured from an approved commercial ASP company. The user privileges are database driven, configurable, and modifiable without needing re-registration. The authentication can be performed via the WEB or via a dedicated VPN.

Benefits

Biometric authentication over the Internet is a robust and efficient method for authenticating remote users and user privileges. Automated biometric authentication will allow access of mission functions/commands and data on a

secure mission server in a seamless and secure manner. A user's biometric signature is unique and cannot be transferred or used by someone else. There are no passwords to steal and user identities cannot be falsified. Also, transactions cannot be repudiated. An automated registration wizard to capture and encode a user's biometric data is used. Routine verification and authentication takes approximately two seconds, via a camera and finger sensor. A user's privileges can be easily configured or reconfigured.